PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-218875
(43)Date of publication of application : 31.07.2003

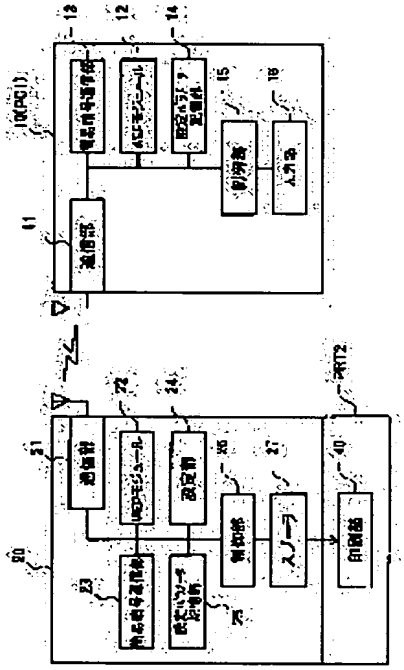
(51)Int.CI. H04L 12/28
H04B 1/06
H04L 9/08
H04Q 7/38

(21)Application number : 2002-009596
(22)Date of filing : 18.01.2002

(71)Applicant : SEIKO EPSON CORP
(72)Inventor : SHIOBARA SUSUMU
GASSHO KAZUTO

(54) SETTING OF PARAMETER FOR RADIO COMMUNICATION APPARATUS

(57)Abstract:
PROBLEM TO BE SOLVED: To avoid leakage of setting parameters when setting to a new radio communication apparatus by the communication apparatus.
SOLUTION: On a side of a radio communication apparatus 10, the setting parameters for establishing connections to existing radio LAN are encrypted in an easy manner and transmitted to a radio print server 20. On a side of the print server 20, the simply encrypted setting parameters transmitted from the communication apparatus 10 are received and decrypted to be set. A simple encryption method and a simple decryption method are previously known between the communication apparatus 10 and the print server 20.



LEGAL STATUS

[Date of request for examination] 25.06.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－218875
（P2003－218875A）
(43)公開日　平成15年７月31日(2003.7.31)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/28	２００	Ｈ０４Ｌ　12/28	２００Ｚ	５Ｊ１０４
Ｈ０４Ｂ　1/06		Ｈ０４Ｂ　1/06	Ｚ	５Ｋ０３３
Ｈ０４Ｌ　9/08			7/26 １０９Ｒ	５Ｋ０６１
Ｈ０４Ｑ　7/38		Ｈ０４Ｌ　9/00	６０１Ｃ	５Ｋ０６７

審査請求　未請求　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願2002－9596(P2002－9596)

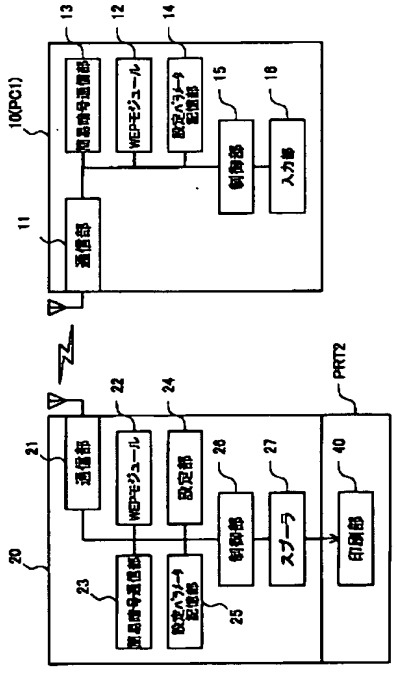
(22)出願日　平成14年１月18日(2002.1.18)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(72)発明者　塩原　進
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内
(72)発明者　合掌　和人
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内
(74)代理人　110000028
特許業務法人明成国際特許事務所

最終頁に続く

(54)【発明の名称】　無線通信装置へのパラメータの設定

(57)【要約】
【課題】　無線通信装置によって新たな無線通信装置の設定を行う際に、設定パラメータの漏洩を回避する。
【解決手段】　無線通信装置１０側で、既存の無線ＬＡＮへの接続を確立するための設定パラメータを簡易暗号化し、無線プリントサーバ２０に送信する。無線プリントサーバ２０側では、無線通信装置１０から送信された簡易暗号化された設定パラメータを受信して復号し、設定する。なお、簡易暗号化および簡易復号の方法は、無線通信装置１０と無線プリントサーバ２０との間で予め既知である。



【特許請求の範囲】

【請求項１】　無線通信装置であって、
無線通信に用いられる設定パラメータを記憶する設定パラメータ記憶部と、
前記設定パラメータの送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、該設定パラメータを暗号化する暗号化部と、
該暗号化された設定パラメータを前記他の無線通信装置に送信する送信部と、
を備える無線通信装置。

【請求項２】　請求項１記載の無線通信装置であって、
前記設定パラメータは、暗号化通信を確立するための鍵情報を含む、
無線通信装置。

【請求項３】　請求項１記載の無線通信装置であって、更に、
前記他の無線通信装置に設定されており、暗号化通信を確立するための鍵情報を入力する鍵入力部を備え、
前記暗号化部は、前記鍵情報を用いて前記暗号化を行う、
無線通信装置。

【請求項４】　無線通信装置であって、
請求項１記載の無線通信装置側で暗号化された設定パラメータを受信する受信部と、
該受信した設定パラメータを、前記暗号化に対応した既知の方法で復号する復号部と、
該復号された設定パラメータに基づいて、前記無線通信の設定を行う設定部と、
を備える無線通信装置。

【請求項５】　請求項４記載の無線通信装置であって、更に、
前記復号部で用いられ、暗号化通信を確立するための鍵情報を乱数的に生成する鍵情報生成部と、
該生成された鍵情報を可視的に出力する出力部と、
を備える無線通信装置。

【請求項６】　請求項４記載の無線通信装置であって、
前記復号部で用いられ、暗号化通信を確立するための鍵情報は、予め設定された情報である、無線通信装置。

【請求項７】　請求項４記載の無線通信装置を備えるプリントサーバ。

【請求項８】　無線通信装置を用いて、他の無線通信装置に対し、無線通信に用いられる設定パラメータを設定する設定方法であって、（ａ）前記設定パラメータを取得する工程と、（ｂ）前記他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、前記設定パラメータを暗号化する工程と、（ｃ）該暗号化された設定パラメータを前記他の無線通信装置に送信する工程と、
を備える設定方法。

【請求項９】　無線通信装置を用いて、他の無線通信装置に対し、無線通信に用いられる設定パラメータを設定するためのコンピュータプログラムであって、
前記設定パラメータを取得する機能と、
前記他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、前記設定パラメータを暗号化する機能と、
該暗号化された設定パラメータを前記他の無線通信装置に送信する機能と、
をコンピュータに実現させるためのコンピュータプログラム。

【請求項１０】　請求項９記載のコンピュータプログラムをコンピュータ読み取り可能に記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、無線通信装置へのパラメータの設定に関する。

【０００２】

【従来の技術】従来、複数のコンピュータやプリンタ等の周辺機器を接続したＬＡＮ（LocalArea Network）が普及している。近年では、接続にケーブルを用いない無線ＬＡＮが普及しつつある。無線ＬＡＮでは、一般に、電波を用いた無線通信を行う無線通信装置が用いられる。この無線ＬＡＮでは、装置間での通信を確立するために、各種パラメータの設定が必要である。更に、第三者へのデータの漏洩を防止するために、暗号化通信が行われる場合もある。暗号化通信では、暗号化用あるいは復号用の鍵情報を各無線通信装置に設定しておく必要がある。既に構築されている無線ＬＡＮに新たな無線通信装置を接続する場合、これらの設定は、一方の無線通信装置から他方の無線通信装置に、無線通信で鍵情報等の設定パラメータを送信することによって行われることがある。

【０００３】

【発明が解決しようとする課題】しかし、設定時は、受信側無線通信装置にとって、暗号化通信を行うための鍵情報は未知であるので、設定パラメータの送受信は、必然的に非暗号化通信で行われていた。このため、設定パラメータが第三者に漏洩するおそれがあり、無線通信におけるセキュリティを確保することができないおそれがあった。

【０００４】かかる課題は、無線プリントサーバなど、パラメータの入力を行うための十分なインタフェースを備えていない無線通信装置への設定時には、特に深刻であった。

【０００５】本発明は、上述の課題を解決するためになされたものであり、無線通信装置によって新たな無線通信装置の設定を行う際に、設定パラメータの漏洩を回避することを目的とする。

【０００６】

【課題を解決するための手段およびその作用・効果】上

述の課題の少なくとも一部を解決するため、本発明では、以下の構成を採用した。本発明の第１の無線通信装置は、無線通信装置であって、無線通信に用いられる設定パラメータを記憶する設定パラメータ記憶部と、前記設定パラメータの送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法で、該設定パラメータを暗号化する暗号化部と、該暗号化された設定パラメータを前記他の無線通信装置に送信する送信部と、を備えることを要旨とする。

【０００７】本発明では、無線通信用の設定パラメータを、送信先となる他の無線通信装置との間で設定パラメータの設定用に予め用意された方法で暗号化して、他の無線通信装置に送信する。こうすることによって、暗号化および復号の方法を知らない第三者への設定パラメータの漏洩を回避することができる。従って、無線通信におけるセキュリティを確保しつつ、新たに設置される無線通信装置に、設定パラメータを、無線通信を介して設定することができる。

【０００８】ここで、「設定パラメータ」とは、例えば、国際標準規格ＩＥＥＥ８０２．１１に基づく無線通信におけるＥＳＳ－ＩＤ、ＷＥＰキー、通信モード、通信チャンネルなどが含まれる。

【０００９】また、「送信先となる他の無線通信装置との間で、前記設定パラメータの送信用に予め用意された方法」とは、例えば、データの配列を２ビットずつずらすなど、予め決められた固有の規則に従って単にデータにスクランブル化をかける方法や、送信側と受信側との双方で既知の秘密鍵（共通鍵ともいう）を用いる方法などが挙げられる。

【００１０】なお、本発明は、Bluetooth（商標）やHomeRF（商標）等の規格に基づいた電波を用いた無線通信装置や、光や音などを用いた無線通信装置にも適用可能である。

【００１１】本発明の第１の無線通信装置において、前記設定パラメータは、暗号化通信を確立するための鍵情報を含むようにすることが好ましい。

【００１２】こうすることによって、鍵情報の漏洩を回避でき、無線通信のセキュリティを向上させることができる。ここで、「鍵情報」とは、データの暗号化および復号に用いられる鍵に関する情報を意味している。鍵情報としては、例えば、国際標準規格ＩＥＥＥ８０２．１１で採用されているＷＥＰ（Wired Equivalent Privacy）と呼ばれる暗号技術で用いられるＷＥＰキー（共通鍵）が挙げられる。鍵情報には、また、先に例示した他の規格に基づいた無線通信に用いられる鍵に関する情報も含まれ得る。

【００１３】本発明の第１の無線通信装置において、更に、前記他の無線通信装置に設定されており、暗号化通信を確立するための鍵情報を入力する鍵入力部を備え、前記暗号化部は、前記鍵情報を用いて前記暗号化を行うようにしてもよい。

【００１４】このように、受信装置側で設定されている鍵情報を、送信側に入力することにより、設定パラメータの送信に鍵情報を用いた暗号化を施すことができるため、単なる規則的なスクランブルをかける方法よりもセキュリティを向上させることができる。受信装置側に設定されている鍵情報は、例えば、予めマニュアル等に記載しておくものとしてもよいし、受信装置側に設けられた表示パネル等に表示させるものとしてもよい。

【００１５】本発明は、上述した本発明の第１の無線通信装置から暗号化された設定パラメータを受信する無線通信装置の発明として構成することもできる。つまり、この無線通信装置は、上述した無線通信装置とサブコンビネーションの関係に相当する。

【００１６】本発明の第２の無線通信装置は、無線通信装置であって、請求項１記載の無線通信装置側で暗号化された設定パラメータを受信する受信部と、該受信した設定パラメータを、前記暗号化に対応した既知の方法で復号する復号部と、該復号された設定パラメータに基づいて、前記無線通信の設定を行う設定部と、を備えることを要旨とする。

【００１７】こうすることによって、無線通信を確立するための設定パラメータを、第三者に漏洩することなく、無線通信を介して受信側無線通信装置に設定することができる。

【００１８】本発明の第２の無線通信装置において、更に、前記復号部で用いられ、暗号化通信を確立するための鍵情報を乱数的に生成する鍵情報生成部と、該生成された鍵情報を可視的に出力する出力部と、を備えるようにしてもよい。

【００１９】「可視的に出力する」とは、受信装置側に設けられた表示パネル等に表示する方法や、受信側無線通信装置に接続された印刷装置によって印刷する方法など視覚に訴える出力態様を意味する。受信側無線通信装置で鍵情報を生成し、可視的に出力することによって、受信側無線通信装置と暗号化通信を確立するための鍵情報を送信側無線通信装置に知らせることができる。送信側無線通信装置側は、出力された鍵情報を用いた暗号化を行うことによって、暗号化通信を確立することができる。

【００２０】なお、本発明の第２の無線通信装置において、前記復号部で用いられ、暗号化通信を確立するための鍵情報は、予め設定された情報であるものとしてもよい。

【００２１】予め設定された鍵情報は、例えば、無線通信装置本体に表示されてもよいし、マニュアルに記載されていてもよい。この受信側無線通信装置側に予め設定された鍵情報を用いた暗号化を、送信側無線装置側で行うことによって、暗号化通信を確立することができる。

【００２２】本発明は、無線通信を利用可能な種々の機

器に適用可能である。例えば、本発明の第２の無線通信装置を備えるプリントサーバとして構成することも可能である。

【００２３】プリントサーバは、通常、十分な入力インタフェースを備えていない。従って、本発明のプリントサーバによって、セキュリティを確保しつつ、上述したパラメータの設定を容易に行うことができる。

【００２４】本発明は、上述の無線通信装置としての構成の他、無線通信に用いられる設定パラメータの設定方法の発明として構成することもできる。また、これらを実現するコンピュータプログラム、およびそのプログラムを記録した記録媒体、そのプログラムを含み搬送波内に具現化されたデータ信号など種々の態様で実現することが可能である。なお、それぞれの態様において、先に示した種々の付加的要素を適用することが可能である。

【００２５】本発明をコンピュータプログラムまたはそのプログラムを記録した記録媒体等として構成する場合には、無線通信装置を駆動するプログラム全体として構成するものとしてもよいし、本発明の機能を果たす部分のみを構成するものとしてもよい。また、記録媒体としては、フレキシブルディスクやＣＤ－ＲＯＭ、光磁気ディスク、ＩＣカード、ＲＯＭカートリッジ、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（ＲＡＭやＲＯＭなどのメモリ）および外部記憶装置などコンピュータが読み取り可能な種々の媒体を利用できる。

【００２６】

【発明の実施の形態】以下、本発明の実施の形態について、実施例に基づき以下の順で説明する。

Ａ．第１実施例：

Ａ１．無線ＬＡＮの構成：

Ａ２．無線通信装置：

Ａ３．パラメータ設定：

Ｂ．第２実施例：

Ｂ１．無線通信装置：

Ｂ２．パラメータ設定：

Ｃ．変形例：

【００２７】Ａ．第１実施例：

Ａ１．無線ＬＡＮの構成：図１は、無線ＬＡＮ１００の構成を示す説明図である。本実施例では、国際標準規格ＩＥＥＥ８０２．１１に基づく無線ＬＡＮを例に説明する。この無線ＬＡＮ１００は、複数のパーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３，ＰＣ４と、プリンタＰＲＴ１と、アクセスポイントＡＰとから構成されている。パーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３，ＰＣ４は、それぞれＣＰＵ、ＲＡＭ、ＲＯＭおよび無線ＬＡＮカードを備えている。更に、パーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３，ＰＣ４それぞれには、無線ＬＡＮカード用のユーティリティソフトがインストールされている。パーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３，ＰＣ４は、それぞれ無線通信装置として機能する。プリンタＰＲＴ１には、無線通信装置を有する無線プリントサーバが接続されている。

【００２８】無線ＬＡＮ１００では、アクセスポイントＡＰを経由して無線通信を行う通信モード（インフラストラクチャ・モード）で各機器間の無線通信を行っている。従って、各パーソナルコンピュータＰＣ１，ＰＣ２，ＰＣ３，ＰＣ４、およびプリンタＰＲＴ１に接続された無線プリントサーバには、それぞれ無線ＬＡＮの各ネットワークをグループ分けするための識別情報であるＥＳＳ－ＩＤや、暗号通信を確立するための鍵情報としてのＷＥＰキーや、通信モード等の各種パラメータが設定されている。共通のパラメータが設定されている機器間でのみ無線暗号化通信が可能である。本実施例では、無線ＬＡＮ１００のＥＳＳ－ＩＤを「ｇｒｏｕｐ」、ＷＥＰキーを「ＡＢＣＤ」とした。

【００２９】ここで、既存の無線ＬＡＮ１００に、新たに無線プリントサーバ２０を備えるプリンタＰＲＴ２を無線接続する。そのためには、無線プリントサーバ２０に上述した各種パラメータを設定する必要がある。本実施例では、無線通信装置１０としてのパーソナルコンピュータＰＣ１から無線通信を介して無線プリントサーバ２０にパラメータを設定する。このようにアクセスポイントＡＰを経由せずに、無線通信装置同士で無線通信を行う通信モードをアドホック・モードと呼ぶ。このアドホック・モードによる無線暗号化通信では、ＷＥＰキーの他に（アドホック・モードでは、ＥＳＳ－ＩＤは使用しない）、無線通信に用いられる電波の周波数を特定する通信チャンネルの設定が必要となる。無線プリントサーバ２０には、通信チャンネルのデフォルト値として「１４」が設定されているものとする。

【００３０】Ａ２．無線通信装置：図２は、本発明の第１実施例としての無線通信装置１０および無線プリントサーバ２０の概略構成を示す説明図である。無線通信装置１０は、通信部１１と、ＷＥＰモジュール１２と、簡易暗号通信部１３と、設定パラメータ記憶部１４と、制御部１５と、入力部１６とを備えている。これらの機能ブロックは、パーソナルコンピュータＰＣ１にパラメータ設定用のユーティリティソフトをインストールすることにより、ソフトウェア的に構築されている。ハードウェア的に構築してもよい。

【００３１】設定パラメータ記憶部１４は、無線ＬＡＮ１００への接続を確立するための各種設定パラメータを記憶している（図１参照）。ＷＥＰモジュール１２は、無線ＬＡＮ１００に接続されているときに、設定パラメータ記憶部１４に記憶されているＷＥＰキー「ＡＢＣＤ」を用いてデータの暗号化および復号を行う。簡易暗号通信部１３は、無線プリントサーバ２０と無線通信を行うときに、データを簡易的に暗号化（以下、簡易暗号化と呼ぶ）する。本実施例では、データの配列を２ビッ

トずつずらすことによって簡易暗号化するものとした。なお、この簡易暗号化の方法は、無線プリントサーバ２０との間で予め既知であるものとする。通信部１１は、暗号化あるいは簡易暗号化されたデータをパケットに分割し、設定パラメータ記憶部１４に記憶されている設定パラメータに基づいて、無線ＬＡＮカードから送信する。つまり、通信部１１は、無線ＬＡＮカードを制御するデバイスドライバとしての機能を有している。入力部１６は、キーボード、マウス等からの指示を入力する。上記各部は、制御部１５によって制御される。

【００３２】無線プリントサーバ２０は、通信部２１と、ＷＥＰモジュール２２と、簡易暗号通信部２３と、設定部２４と、設定パラメータ記憶部２５と、制御部２６と、スプーラ２７とを備えている。通信部２１は、無線通信装置１０から送信されたパケットを受信し、結合する。ＷＥＰモジュール２２は、無線ＬＡＮ１００に接続されているときに、ＷＥＰキーを用いてデータの暗号化および復号を行う。簡易暗号通信部２３は、無線通信装置１０の簡易暗号通信部１３に対応した簡易的な復号（以下、簡易復号と呼ぶ）を行う。本実施例では、データの配列を２ビットずつ簡易暗号通信部１３と逆方向にずらすことによって、簡易復号を行う。設定パラメータ記憶部２５は、無線通信用の設定パラメータを記憶しており、当初は、図１に示した通り、「ＥＳＳ－ＩＤ：なし、ＷＥＰキー：なし」などの設定が記憶されている。設定部２４は、設定パラメータ記憶部２５の内容を、簡易復号された設定パラメータの内容に更新する。なお、設定パラメータ記憶部２５には、デフォルト値の設定パラメータと、新規の設定された設定パラメータとが別々に記憶されるようにしてもよい。スプーラ２７は、印刷ジョブの保持、管理、印刷部４０への出力など、プリントサーバとしての主機能を実現する。

【００３３】Ａ３．パラメータ設定：図３は、第１実施例における設定パラメータの設定工程を示す説明図である。図の右側に無線通信装置１０での処理を示し、左側に無線プリントサーバ２０での処理を示した。まず、無線通信装置１０側で、無線プリントサーバ２０との無線通信を確立するための通信設定を行う（ステップＳ１００）。つまり、無線通信装置１０の設定を図１に示した無線プリントサーバ２０の設定パラメータに一致させる。但し、この時点で、無線ＬＡＮ１００に接続するための設定パラメータも、無線プリントサーバ２０に送信すべき情報として設定パラメータ記憶部１４に保持されている。無線プリントサーバ２０の設定を行うためのユーティリティソフトによって、この設定パラメータを修正可能としてもよい。

【００３４】次に、ユーザによって設定パラメータの送信コマンドが入力されると、簡易暗号通信部１３は、既存の設定パラメータを簡易暗号化する（ステップＳ１１０）。そして、通信部１１は、簡易暗号化された設定データをパケットに分割し、無線ＬＡＮカードから無線プリントサーバ２０に送信する（ステップＳ１２０）。

【００３５】無線プリントサーバ２０側では、無線通信装置１０から送信された簡易暗号化された設定パラメータを通信部２１で受信し（ステップＳ１３０）、簡易暗号通信部２３で簡易復号する（ステップＳ１４０）。そして、設定部２４が、復号されたデータに基づいてＷＥＰキーを「ＡＢＣＤ」に設定するなど設定パラメータ記憶部２５の内容を更新設定する（ステップＳ１５０）。以上の工程を経て、無線プリントサーバ２０は、無線通信装置１０から受信した設定パラメータを用いて既存の無線ＬＡＮ１００に接続することが可能となる。

【００３６】以上説明した第１実施例の無線通信装置１０および無線プリントサーバ２０によれば、設定パラメータを暗号化して無線プリントサーバ２０に送信することができるので、設定パラメータの漏洩を回避でき、無線ＬＡＮ１００のセキュリティを確保することができる。

【００３７】Ｂ．第２実施例：

Ｂ１．無線通信装置：図４は、本発明の第２実施例としての無線通信装置１０Ａおよび無線プリントサーバ２０Ａの概略構成を示す説明図である。無線通信装置１０Ａは、第１実施例の無線通信装置１０と異なり、簡易暗号通信部１３を備えていない。この代わりに、入力部１６Ａが、無線プリントサーバ２０Ａとの暗号化通信を確立するためのＷＥＰキーを入力する機能を有している。このＷＥＰキーは、後述する無線プリントサーバ２０Ａで生成されるものであり、無線ＬＡＮ１００において用いられるＷＥＰキー「ＡＢＣＤ」とは異なる。設定パラメータ記憶部１４Ａは、既存のＷＥＰキー「ＡＢＣＤ」と新たに入力されるＷＥＰキーとを別々に保持することができる。ＷＥＰモジュール１２Ａは、無線ＬＡＮ１００に接続されているときには、設定パラメータ記憶部１４に記憶されている既存のＷＥＰキー「ＡＢＣＤ」を用いて暗号化および復号を行い、無線プリントサーバ２０Ａと無線通信を行うときには、新たに入力されたＷＥＰキーを用いて暗号化を行う。この他は、第１実施例の無線通信装置１０と同じである。

【００３８】無線プリントサーバ２０Ａは、第１実施例の無線プリントサーバ２０と異なり、簡易暗号通信部２３を備えていない。この代わりに、ＷＥＰキー生成部２８と、スイッチ２９とを備えている。ＷＥＰキー生成部２８は、ユーザがスイッチ２９を操作することによって、ＷＥＰキーを乱数的に生成する。ここで、ＷＥＰキー生成部２８で生成されたＷＥＰキーは、「ＥＦＧＨ」であるものとする。ＷＥＰキー「ＥＦＧＨ」は、スプーラ２７に送られ、プリンタＰＲＴ２の印刷部４０によって印刷される。また、ＷＥＰキー生成部２８は、生成されたＷＥＰキー「ＥＦＧＨ」を設定パラメータ記憶部２５に記憶させる。この結果、ＷＥＰモジュール２２は、

無線通信装置１０Ａと無線通信を行うときには、ＷＥＰキー「ＥＦＧＨ」を用いて通信を行うことが可能となる。この他は、第１実施例の無線プリントサーバ２０と同じである。

【００３９】Ｂ２．パラメータ設定：図５は、第２実施例における設定パラメータの設定工程を示す説明図である。図の右側に無線通信装置１０Ａでの処理を示し、左側に無線プリントサーバ２０Ａでの処理を示した。まず、無線プリントサーバ２０ＡのＷＥＰキー生成部２８でＷＥＰキーを生成し（ステップＳ２００）、プリンタＰＲＴ２によって印刷出力する（ステップＳ２１０）。これらの工程は、先に説明したように、ユーザがスイッチ２９を操作することによって行われる。

【００４０】無線通信装置１０Ａ側では、第１実施例と同様に、無線プリントサーバ２０Ａとの無線通信を確立するための通信設定を行う（ステップＳ２２０）。更に、ユーザが無線プリントサーバ２０Ａ側で印刷出力されたＷＥＰキー「ＥＦＧＨ」を入力する（ステップＳ２３０）。次に、ユーザによって設定パラメータの送信コマンドが入力されると、ＷＥＰモジュール１２Ａは、既存の無線ＬＡＮ１００への接続を確立するための既存の設定パラメータを、入力されたＷＥＰキー「ＥＦＧＨ」を用いて暗号化する（ステップＳ２４０）。そして、通信部１１は、暗号化された設定パラメータをバケットに分割し、無線ＬＡＮカードから無線プリントサーバ２０Ａに送信する（ステップＳ２５０）。

【００４１】無線プリントサーバ２０Ａ側では、無線通信装置１０Ａから送信された暗号化された設定パラメータを通信部２１で受信し（ステップＳ２６０）、ＷＥＰキー生成部２８で生成されたＷＥＰキー「ＥＦＧＨ」を用いて復号する（ステップＳ２７０）。そして、設定部２４が、復号されたデータに基づいてＷＥＰキーを「ＡＢＣＤ」に変更するなど設定パラメータ記憶部２５の内容を更新設定する（ステップＳ２８０）。以上の工程を経て、無線プリントサーバ２０Ａは、無線通信装置１０Ａから受信した設定パラメータを用いて既存の無線ＬＡＮ１００に接続することが可能となる。

【００４２】以上説明した第２実施例の無線通信装置１０Ａおよび無線プリントサーバ２０Ａによれば、無線プリントサーバ２０Ａで乱数的に生成されたＷＥＰキーを用いて設定パラメータを暗号化して無線プリントサーバ２０に送信することができるので、設定パラメータの漏洩を回避でき、無線ＬＡＮ１００のセキュリティを確保することができる。

【００４３】Ｃ．変形例：以上、本発明のいくつかの実施の形態について説明したが、本発明はこのような実施の形態になんら限定されるものではなく、その要旨を逸脱しない範囲内において種々なる態様での実施が可能である。例えば、以下のような変形例が可能である。

【００４４】Ｃ１．変形例１：上記第１実施例では、既存の設定パラメータの暗号化に単純なスクランブルを用いたが、共通鍵方式による暗号化を用いるものとしてもよい。ここで用いられる共通鍵は、第２実施例と同様の手法により、無線通信装置１０側に入力すればよい。

【００４５】Ｃ２．変形例２：上記第２実施例では、ＷＥＰキー生成部２８を備えているが、これを備えないようにしてもよい。この場合、無線プリントサーバ２０Ａの製造時にデフォルト値として設定パラメータ記憶部２５に記憶されたＷＥＰキーを用いるものとしてもよい。デフォルト値として設定されたＷＥＰキーは、第２実施例のように印刷出力してもよいし、装置本体やマニュアル等に記載しておくものとしてもよい。

【００４６】Ｃ３．変形例３：上記第２実施例では、ＷＥＰキー生成部２８で生成されたＷＥＰキーを印刷により出力するものとしたが、これに限られず、ユーザが知ることができるように出力すればよい。従って、例えば、無線プリントサーバ２０Ａや、プリンタＰＲＴ２に表示パネルを設けて表示するようにしてもよいし、音声によって出力するようにしてもよい。

【００４７】Ｃ４．変形例４：上記実施例では、本発明を国際標準規格ＩＥＥＥ８０２．１１に基づく無線通信装置に適用した場合について説明したが、これに限られない。本発明は、一般に、一方の無線通信装置から他方の無線通信装置へ、無線通信に用いられる設定パラメータを設定するものであるから、例えば、Bluetooth（商標）やHomeRF（商標）等の規格に基づいた無線通信装置にも適用可能である。この場合、各規格に対応した暗号化技術を適用すればよい。

【００４８】Ｃ５．変形例５：上記実施例では、電波を用いた無線暗号通信を例に説明したが、これに限られず、例えば、光や音などを媒体とした無線通信を行う無線通信にも適用可能である。

【図面の簡単な説明】

【図１】無線ＬＡＮ１００の構成を示す説明図である。

【図２】本発明の第１実施例としての無線通信装置１０および無線プリントサーバ２０の概略構成を示す説明図である。

【図３】第１実施例における設定パラメータの設定工程を示す説明図である。

【図４】本発明の第２実施例としての無線通信装置１０Ａおよび無線プリントサーバ２０Ａの概略構成を示す説明図である。

【図５】第２実施例における設定パラメータの設定工程を示す説明図である。

【符号の説明】

１０、１０Ａ…無線通信装置
１１…通信部
１２、１２Ａ…ＷＥＰモジュール
１３…簡易暗号通信部
１４、１４Ａ…設定パラメータ記憶部

11

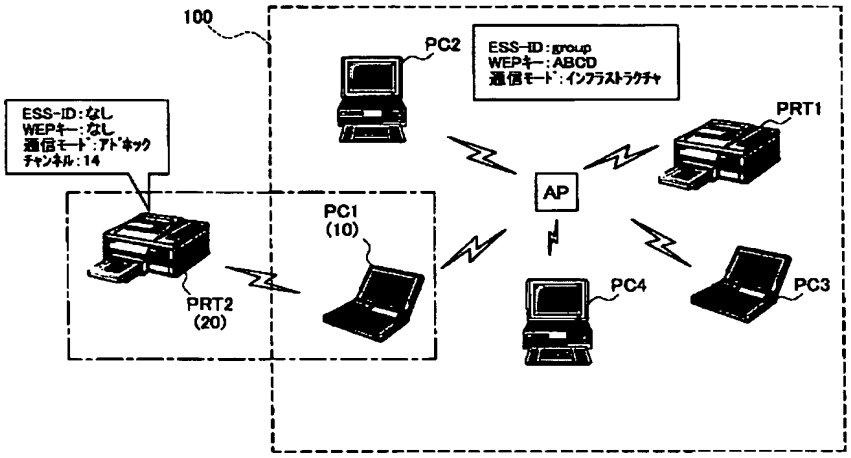
１５…制御部
１６、１６Ａ…入力部
２０、２０Ａ…無線プリントサーバ
２１…通信部
２２…ＷＥＰモジュール
２３…簡易暗号通信部
２４…設定部

12

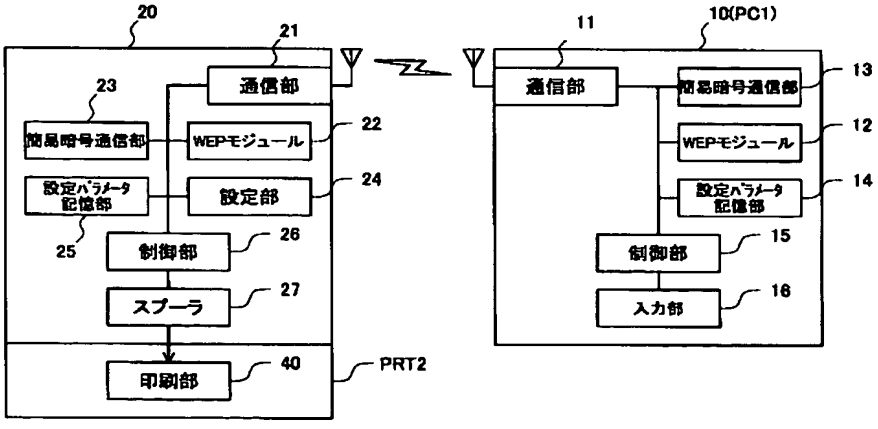
＊２５…設定パラメータ記憶部
２６…制御部
２７…スプーラ
２９…スイッチ
４０…印刷部
１００…無線ＬＡＮ

＊

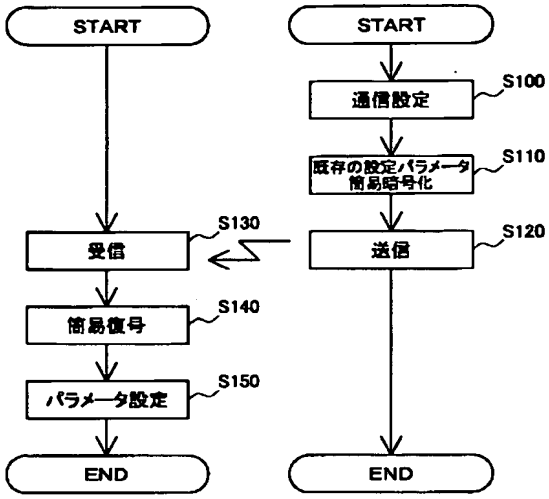
【図１】



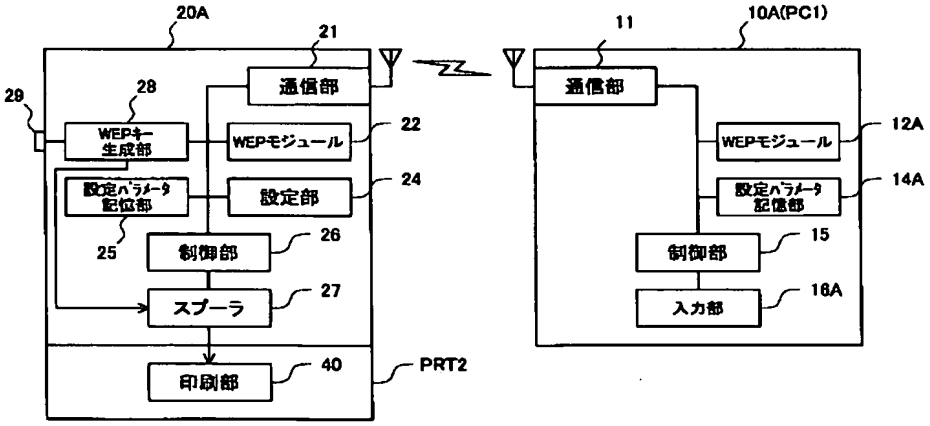
【図２】



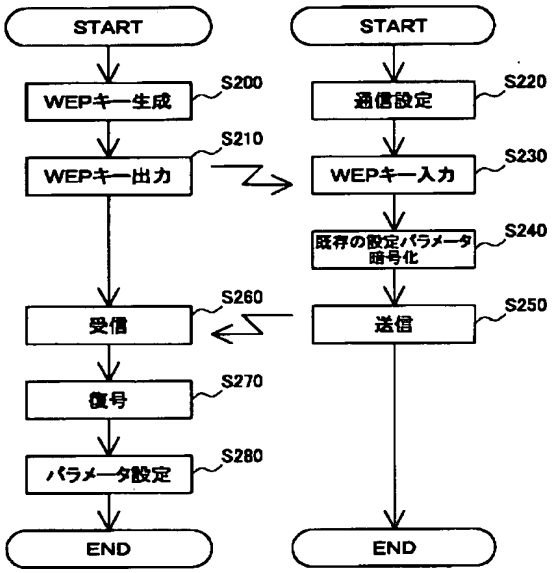
【図３】


START
START
通信設定
S100
既存の設定パラメータ
簡易暗号化
S110
受信
S130
送信
S120
簡易復号
S140
パラメータ設定
S150
END
END

【図４】


20A
21
11
10A(PC1)
通信部
通信部
29
28
WEPキー
生成部
WEPモジュール
22
WEPモジュール
12A
設定パラメータ
記憶部
設定部
24
設定パラメータ
記憶部
14A
25
制御部
26
制御部
15
スプーラ
27
入力部
16A
印刷部
40
PRT2

【図５】



フロントページの続き

Ｆターム(参考) 5J104 AA01 PA07
5K033 AA08 DA17
5K061 AA05 AA09 AA15
5K067 AA30 BB21 DD17 EE02 EE10
EE12 HH23 HH36 KK13 KK15